CLARKSON LAW FIRM, P.C
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (CA SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood (SBN 149343)
tblood@bholaw.com
Jennifer L. MacPherson (SBN 202021)
jmacpherson@bholaw.com
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: (619) 338-1100
Fax: (619) 338-1101

COTCHETT, PITRE & McCARTHY LLP
Thomas E. Loeser (SBN 202724)
tloeser@cpmlegal.com
Karin B. Swope (*PHV forthcoming*)
kswope@cpmlegal.com
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577

ROSSBACH LAW, P.C.
William A. Rossbach (SBN 1338)
bill@rossbachlaw.com
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Tel: (406) 543-5156

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROBERT JONES, and KATHY MARTIN, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

SNOWFLAKE, INC.,

Defendant.

Case No: 3:24-cv-5323

CLASS ACTION COMPLAINT

1. NEGLIGENCE
2. NEGLIGENCE PER SE
3. BREACH OF FIDUCIARY DUTY
4. UNJUST ENRICHMENT
5. BREACH OF IMPLIED CONTRACT
6. BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
7. VIOLATION OF THE CCPA, Cal. Civ. Code §§ 1798.100, *et seq.*
8. VIOLATION OF THE UCL, Cal. Bus. & Prof. Code §§ 17200, *et seq*

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Plaintiffs Robert Jones and Kathy Martin (collectively, "**Plaintiffs**") individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "**Complaint**"), and allege the following against Defendant Snowflake, Inc. ("**Snowflake**" or "**Defendant**"), based upon personal knowledge with respect to themselves and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similar situated individuals' personal identifiable information ("**PII**"), including but not limited to full names, addresses, email addresses, social security numbers, auto insurance information ("**AII**"), including but not limited to driving records and other details involved in insurance premium calculations, personal financial information ("**PFI**") including but not limited to credit card numbers and purchase histories, and online tracking information ("**OTI**"), including but not limited to pixel tracking data (browsing histories), device IP addresses and other sensitive information. This information collectively referred to as "**Private Information**").

2. This class action arises out of Snowflake's failure to secure its cloud storage systems, enabling third party criminals to access and misuse highly sensitive PII from Snowflake's cloud storage and systems (the "**Data Breach**").

3. Snowflake provides digital warehouses, known as the "Snowflake Data Cloud," for its thousands of clients around the world, and as a result has access to, stores, and maintains huge datasets of Private Information of its corporate clients' customers and employees. For the purposes of this action, Snowflake's corporate clients are entities that contracted with Snowflake to store confidential files of their customers and employees. Snowflake's corporate clients include, but are not limited to, AT&T, Ticketmaster, Mastercard, Nielsen, Novartis, PepsiCo, Siemens, Advanced Auto Parts, Santander Bank, Allstate Insurance, Anheuser-Busch, Mitsubishi, Neiman Marcus, Doordash, HP, Instacart, Capital One, JetBlue, Pitney Bowes, Progressive, State Farm, NBC Universal, and many others.[1]

[1] *See, Leaders Choose Snowflake*, SNOWFLAKE (N.D.), https://www.snowflake.com/en/customers/all-customers/ (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

4. Snowflake's corporate clients paid a fee to Snowflake for Snowflake's data cloud storage and services. The fee was at least in part paid to maintain security features surrounding Snowflake's data storage. As a result, Snowflake was required to secure its cloud storage systems, on which its corporate clients stored sensitive information and files containing Private Information of millions of individuals – their customers and employees (the affected Plaintiffs and Class Members).

5. Due to the Data Breach, Plaintiffs and Class Members[2] suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their Private Information. As a result of this Data Breach, around 165 of Snowflake's corporate clients' customers' and employees' sensitive information was exposed and misused.[3]

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect the Private Information exfiltrated. Snowflake could have easily prevented the Data Breach by requiring all users to use multi-factor authentication, allowing the companies that store information on its data cloud services to enforce multi-factor authentication ("**MFA**") for the users, requiring all accounts to regularly update their passwords (as any reasonably prudent cloud service provider would in this industry), monitor suspicious activities on its data clouds, implementing protocols for detection of unusual activities associated with unauthorized access, limiting access to its networks/cloud services to only necessary users, monitor infostealer marketplaces for compromised credentials, preventing access to the platforms/clouds from suspicious accounts, following the basic industry standards for maintaining reasonable security measures of its cloud. Had even some of these basic features been enabled (such as allowing administrator enforcement, i.e. that Snowflake's corporate clients themselves could require MFA access to their respective Data Clouds), this Data Breach would have

[2] "Class Members" defined *infra* at ¶ 76

[3] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion. (last visited Aug. 16, 2024).

been prevented.

7. In fact, an investigation by Google-owned cybersecurity firm Mandiant revealed that the threat campaign orchestrated by the uncharacterized threat actor group "UNC5537" was successful because, "the impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password."[4] In other words, had Snowflake enabled multi-factor authentication for all users of its databases, this Data Breach would have been prevented. Because Snowflake has control over its systems on which it stores the sensitive data and files of its corporate clients (and in turn, the affected victims of the data breach – Plaintiffs and the Class).

8. Plaintiffs, and everyone whose data was auctioned off to criminals, are now victims of identity theft—as any combination of this Private Information will forever subject them to being targets of cyber-attacks. The Private Information exfiltrated is highly substantial and will affect the victims of the Data Breach, Plaintiffs and the putative class, forever. Even years from now, Plaintiffs and other victims will be subject to cyber-attacks, and phishing scams.

9. The Data Breach was a direct result of Snowflake's failure to implement adequate and reasonable cybersecurity procedures and protocols, consistent with the industry standard, "necessary" to protect Private Information from the foreseeable threat of a cyberattack. Snowflake was fully aware that it was responsible for enabling MFA-related security features (as well as other security protocols discussed above) to protect the Private Information of millions of customers and employees of the companies/clients whom it serviced.

10. Any entity that prioritizes the security of sensitive information, employing necessary security measures, would ensure that it and all parties it contracts with had secure procedures surrounding its Data Cloud environment. Snowflake did not do so, electing to disable (or not enable) even the basic security features related to the MFA – disallowing companies it services to enable and enforce the MFAs.

11. MFA is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (i.e., a username/password and

[4] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

confirmation link sent via email). MFA is "a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords."[5]

12. ShinyHunters boasted to journalists that the Data Breach (which affected customers and/or employees of 165 companies) was enabled by Snowflake's lack of MFA enforcement.[6] Snowflake inexplicably leaves the option to enable MFA up to individual users, so data environments can be compromised through "weak links" – users who elect to not enroll in MFA for their accounts.[7]

13. MFA administrator enforcement is the industry standard, according to Ofer Maor, cofounder and Chief Technology Officer of data security investigation firm Mitiga.[8] He notes that "most SaaS (soft-as-a-service) vendors, once deployed as an enterprise solution, allow administrators to enforce MFA… they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it." A data security firm's principal simply noted it is "surprising that the built-in account management within Snowflake doesn't have more robust capabilities like the ability to enforce MFA.[9]

14. Snowflake, as a data cloud service provider, is aware that certain basic security measures could lead to a substantial loss of sensitive information – one of which is implementing MFA requirements, enabling administrator controls to mandate MFA for its users, yet it took no remedial or preemptive measures to ensure that the sensitive information located on its clouds was protected. By way of example, implementing a policy to enable MFA and even allowing the companies who use Snowflake's cloud servers to enforce MFA features would have prevented this Data Breach.

[5] Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, INFORMATIONWEEK (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say. (last visited Aug. 16, 2024).

[6] *Id.*

[7] *FAQ: Multi-Factored Authentication (MFA)*, SNOWFLAKE (August 5, 2023), https://community.snowflake.com/s/article/MFA-FAQs. (last visited Aug. 16, 2024).

[8] Solomon Klappholz, *With Hundreds of Snowflake Credentials Published on the Dark Web, It's Time for Enterprises to Get MFA in Order*, ITPRO (June 7, 2024), https://www.itpro.com/security/cyber-attacks/with-hundreds-of-snowflake-credentials-published-on-the-dark-web-its-time-for-enterprises-to-get-mfa-in-order. (last visited Aug. 16, 2024).

[9] Snider, *supra* note 5

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

15. Snowflake received a financial benefit – a fee for its services which included storing and protecting its data cloud servers to ensure that Plaintiffs and class members' Private Information would be protected. Snowflake assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs and Class Members' Private Information against unauthorized access and disclosure. It was aware that the large data files stored on its servers contain sensitive information about millions of individuals – the clients/employees of thousands of companies with whom Snowflake contracted. Snowflake's responsibility was to protect their cloud servers and the sensitive files stored on their servers. At least a partial (if not full) payment for Snowflake's services was attributed to protecting the files and sensitive information on its cloud platforms.

16. Snowflake further had a duty to adequately safeguard this Private Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "**FTC Act**").

17. Snowflake breached its duties and disregarded the rights of Plaintiffs and the Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard individuals' (whose information it was required to protect located on its servers) Private Information; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing to follow applicable, required, and proper protocols, policies, and procedures regarding the encryption of data.

18. As a result of Snowflake's inadequate security and breach of their duties and obligations, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unauthorized criminal third party – the sensitive files of millions of individuals were posted on dark web for sale to other criminals. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) diminution in value and/or lost value of Private Information, a form of property that Defendant obtained from Plaintiffs and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (iii) opportunity costs associated with attempting to mitigate the actual consequences

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs and Class Members' Private Information; (v) the continued and certain increased risk that the Private Information that remains in Snowflake's possession is subject to further unauthorized disclosure for so long as Snowflake fail to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; and (vi) theft of their Private Information and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

19. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiffs and Class Members' sensitive and confidential Private Information remains in Snowflake's possession. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft. The aggregate data compromised in the Data Breach, taken as a whole, includes but is not necessarily limited to ***full names, addresses, email addresses, social security numbers, driving records and other details involved in insurance premium calculations, credit card numbers and purchase histories, pixel tracking data (browsing histories) and device IP addresses***.

20. Snowflake disregarded the rights of Plaintiffs and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

21. In addition, Defendant failed to properly monitor its computer network and systems that housed the Private Information. Had it properly monitored these electronic and cloud-based systems, it would have discovered the intrusion sooner or prevented it altogether.

22. The security of Plaintiffs and Class Members' identities is now at substantial risk because of Snowflake's wrongful conduct as the Private Information that Snowflake maintained on

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

its cloud servers is now in the hands of data thieves. This present risk will continue for the course of their lives.

23. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes.

24. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

25. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because they exposed other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

26. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained.

27. Plaintiffs, on behalf of themselves and all other Class Members, bring claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Snowflake's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

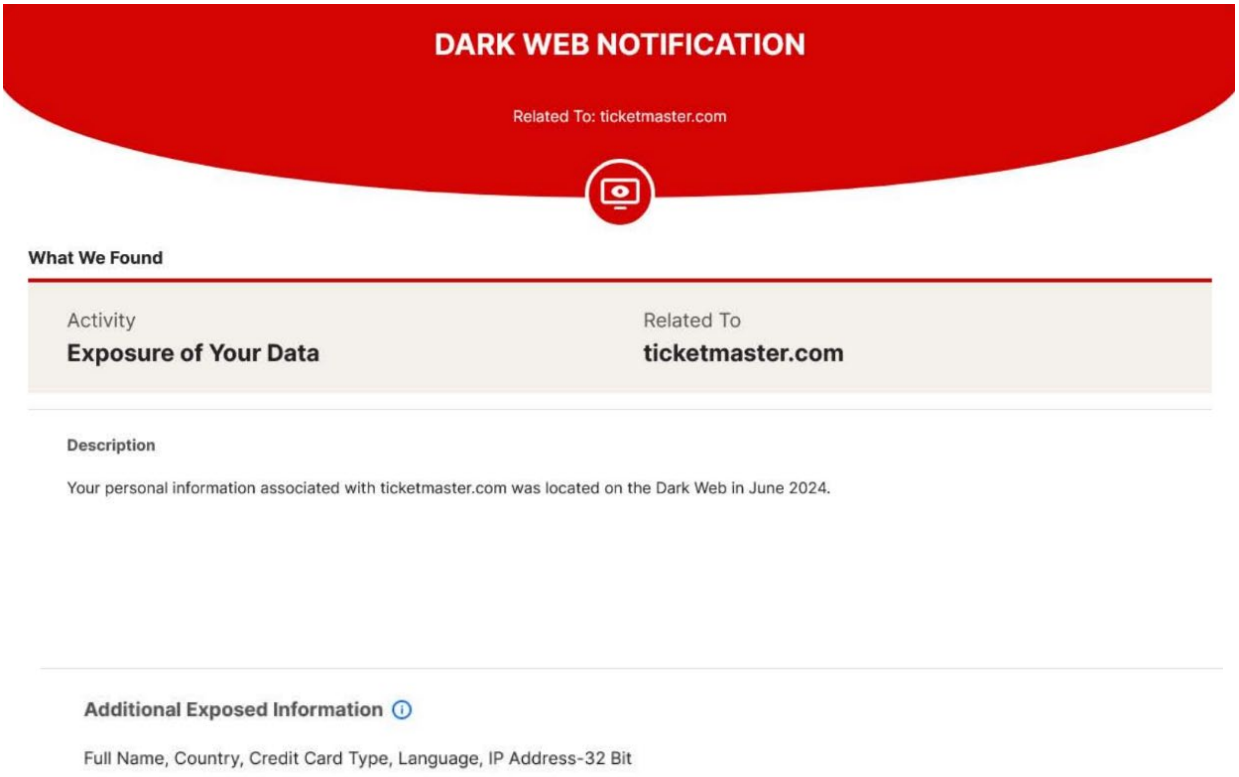
Plaintiff Robert Jones ("Plaintiff Jones" or "Plaintiff")

28. Plaintiff Jones is a citizen of the state of California. At all relevant times, Plaintiff has resided in the county of Los Angeles.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

29. Plaintiff Jones has been a customer of Snowflake corporate client Ticketmaster. Ticketmaster is one of the 165 companies who entrusted Snowflake with the security and protection of the cloud servers on which Plaintiff Jones sensitive information was stored. Plaintiff Jones provided his Private Information to Ticketmaster and as a result to Snowflake, including his credit card. In receiving and maintaining his Private Information for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Jones's Private Information. Defendant, however, did not take proper care of Plaintiff Jones's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate cybersecurity measures.

30. Plaintiff Jones received notice of the Data Breach on July 3, 2024, from his cybersecurity monitoring service Norton. Plaintiff Jones is deeply concerned that his Private Information is now available on the dark web, including, but not necessarily limited to, his *full name, address, credit card information, and IP address* (a true and correct screenshot of Plaintiff Jones's Norton Data Breach Notification immediately follows):



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

31. Since learning about the Data Breach, Plaintiff Jones anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff Jones will need to review for fraudulent activity and closely monitor his financial information.

32. Plaintiff Jones suffers a substantially increased risk of fraud, identity theft, and data misuse resulting from his Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

33. Plaintiff Jones has a continuing interest in ensuring that his Private Information, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kathy Martin ("Plaintiff Martin" or "Plaintiff")

34. Plaintiff Martin is a citizen of the State of Texas. At all relevant times, Plaintiff has resided in the county of Irving, Texas.

35. Plaintiff Martin has been a customer of Snowflake corporate client Ticketmaster. Ticketmaster is one of the 165 companies who entrusted Snowflake with the security and protection of the cloud servers on which Plaintiff Martin's sensitive information was stored. Plaintiff provided her Private Information to Ticketmaster and as a result to Snowflake, including her credit card. In receiving and maintaining her Private Information for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Martin's Private Information. Defendant, however, did not take proper care of Plaintiff Martin's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate cybersecurity measures.

36. Plaintiff Martin is deeply concerned by the Data Breach because she frequently uses Ticketmaster to purchase concert tickets. Plaintiff Martin continues to worry about her Private Information, as it is readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

37. Since learning about the Data Breach, Plaintiff Martin anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff Martin will need to review for fraudulent activity and closely monitor her financial information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

38. Plaintiff Martin suffers a substantially increased risk of fraud, identity theft, and data misuse resulting from her Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

39. Since the Data Breach, Plaintiff Martin has experienced unauthorized attempts to access her email, unauthorized transfer of her Ticketmaster purchases to other persons, an increase in spam calls and phishing attempts, unauthorized access to her social media and other personal accounts, and emotional distress.

40. Plaintiff Martin has a continuing interest in ensuring that her Private Information, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Defendant

41. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

42. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[10]

43. Snowflake's Data Cloud platform is used globally, with 9,437 institutions trusting Snowflake to manage and store customers' data.[11]

44. Defendant maintains main offices and employees who specifically oversee and handle data privacy, data policies, and make data-driven decisions in San Mateo, California. Defendant's co-founders both work in this District,[12] from which they made and continue to make decisions concerning Snowflake's cloud, security, and other issues. Defendant's Vice President of Information Security, responsible for "building and maturing robust Information Security programs," works in

[10] *Form 10-Q Quarterly Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited Aug. 16, 2024).

[11] *Form 10-K Annual Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited Aug. 16, 2024).

[12] *Benoit Dageville,* LINKEDIN, [LinkedIn Profile] https://www.linkedin.com/in/benoit-dageville-3011845/ (last visited Aug. 16, 2024); *Thierry Cruanes*, LinkedIn, [LinkedIn Profile] https://www.linkedin.com/in/thierry-cruanes-3927363/ (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

this District.[13] Defendant's Chief Information Officer and Data Officer works in this District.[14] Despite relocating its nominal "headquarters" to Bozeman, MT in 2021, Defendant's San Mateo office remains the nexus from which Defendant's data-related privacy policies, protections, important decisions impacting consumers' data, and other data driven decision making processes are developed and authorized.[15] In fact, Defendant regularly hosts its "Snowflake Summit" in the Moscone Convention Center, in San Francisco.[16] The Snowflake Summit is a series of training and certification sessions where, among other things, "privacy-preserving collaboration" is taught.[17] Snowflake will host another Summit in San Francisco in 2025.[18]

45. Due to the nature of the services Snowflake provides, it receives and is entrusted with securely storing Plaintiffs and Class Members' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. As a contracting party entrusted with millions of Class Members' Private Information, Snowflake was expected to provide confidentiality and adequate security for the data it collected in accordance with its corporate clients' promises and disclosures and is expected to comply with statutory privacy requirements.

JURISDICTION AND VENUE

46. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs,

[13] *Brad Jones*, LinkedIn, [LinkedIn Profile] https://www.linkedin.com/in/brad-jones-6963b14/ (last visited Aug. 16, 2024)

[14] *Sunny Bedi*, LinkedIn, [LinkedIn Profile] https://www.linkedin.com/in/sunny-bedi-b73129/ (last visited Aug. 16, 2024)

[15] Stephen Council, *2 Years After Pulling HQ From Bay Area, Snowflake Reportedly Eyes Huge New Office*, SFGATE (Aug. 16, 2023), https://www.sfgate.com/tech/article/snowflake-new-office-real-estate-18299429.php (last visited Aug. 16, 2024).

[16] N.A., *Snowflake Summit 2024*, DATANAMI, [Event Page] https://www.datanami.com/event/snowflake-summit-2024/#:~:text=Snowflake%20is%20coming%20home%20to,Data%20Cloud%20has%20to%20offer (last visited Aug. 16, 2024).

[17] *Id.*

[18] N.A., *Summit 2025 Save the Date*, SNOWFLAKE, https://www.snowflake.com/summit/save-the-date/ (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 | F: (213) 788-4070 | clarksonlawfirm.com

and (iii) there is minimal diversity because at least one Plaintiff (here, both Plaintiffs, residents of TX and CA) and Defendant (MT, DE) are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

47. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's decision making processes affecting data and privacy stem from its San Mateo offices, Defendant markets and sells products and services in this District, Defendant gains revenue and profits from doing business in this District, Defendant enters into contracts with its corporate clients in this district, Class Members affected by the breach reside in this District, Defendant has a corporate office in this District, and Defendant employs numerous people (including top-level leaders) in this District, a number of whom work specifically on making decisions regarding the data privacies and handling of consumers' data.

48. Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California, and the decisions affecting consumers data and privacy stem from the San Francisco offices. Defendant is authorized to do and is doing business in California, Defendant advertises and solicits business in California, Defendant has a showroom store in California, and Defendant has corporate offices in California. Defendant has purposefully availed itself to the protections of California law and should reasonably expect to be hauled into court in California for harm arising out of its pervasive contacts with California.

FACTUAL BACKGROUND

I. The Data Breach, and Defendant's Unsecure Data Management.

49. As a direct result of Defendant's failure to implement basic security measures, millions of Americans have had their PII made available on the dark web to be purchased by criminals. Cybersecurity firms, journalists, and threat actors have claimed that 165 Snowflake customers' data had been exfiltrated. At least the following confidential of the following companies have been released as a result of Snowflake's security failures:[19]

- **Ticketmaster**. On May 28, 2024, threat actors posted that 1.4 terabytes of Ticketmaster

[19] Mandiant, *supra* note 4.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

customers' Private Information were available for purchase on the hacking website Breach Forums.[20] The notorious hacking group ShinyHunters offered the trove of Plaintiff's and Class Members' Private Information for $500,000. Ticketmaster, and its parent company Live Nation has confirmed the loss of files was as a result of Snowflake's Data Breach which occurred on May 20, 2024.[21] The lost information included "560 million customers [sic] full details (name, address, email, phone) – Ticket sales, event information, order details – CC [credit card] detail [sic] – customer, last 4 of card, expiration date. Customer fraud details – much more."[22]

- **Advance Auto Parts**. Likewise, Snowflake breach also affected the employees and customers of Advanced Auto parts. The released information included sensitive employee data. On June 5, 2024, the threat actor known by their online handle "Sp1d3r," posted on a hacking forum that 3 Terabytes of AAP's data was up for sale. The hacker confirmed that the data was exfiltrated from "AAP Snowflake" and included: "380M customer profiles (name, email, mobile, phone, address, more) – 140M customer orders – 44M Loyalty/Gas card numbers (with customer details) – 358K Employees – Sales history – Employment candidate info with SSNs, drivers' license numbers, demographic details – Transaction tender details – Over 200 tables of data!"[23] This trove of information is available for $1.5 million USD.
- **Neiman Marcus**. As a result of Snowflake's failure to protect information, its customers – clients of Neiman Marcus, stored on its data cloud, were also affected. Spid3r posted their sensitive information for sale, confirming that names, emails, addresses, dates of birth, last four digits of social security numbers, 50 million customer emails and IP

[20] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k,* HACKREAD (May 29, 2024), https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/. (last visited Aug. 16, 2024).

[21] *Form 8-K Current Report for Live Nation Entertainment, Inc.*, SEC.GOV, https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm?=7194ef805fa2d04b0f7e8c9521f97343 (last visited Aug. 16, 2024).

[22] *Id.*

[23] Sergiu Gatlan, *Advance Auto Parts Stolen Data For Sale After Snowflake Attack*, BLEEPINGCOMPUTER (June 5, 2024) https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/ (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

addresses, and 70 million customer transaction data were included in this dataset.[24] Neiman Marcus so far has confirmed that only 64,472 people were impacted, which appears to be inaccurate given the criminal's posted information for sale.

- **Lending Tree**. As a result of Snowflake's failure to protect information, its customers – clients of Lending Tree were also affected. Sp1d3r confirmed that it exfiltrated 190 million customers' personal data and "3 billion pixel data" including "full customer details, partial CC details (only middle 5 numbers masked), auto history, driving records, personal background information needed for insurance quotes, 3 billion tracking pixels (contains PII and IP/online tracking details)." [25] Sp1d3r furthered sweetened its trove of data by including some of Lending Tree's subsidiary's (QuoteWizard) clients, which include the largest auto insurance companies in the United States, such as Allstate, State Farm, Progressive and Farmers Insurance.[26]

II. Defendant's Duty to Safeguard Private Information

50. Private Information is a valuable property right.[27] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[28] It is estimated that American

[24] Lawrence Abrams, *Neiman Marcus Confirms Data Breach After Snowflake Account Hack*, BLEEPINGCOMPUTER (June 28, 2024), https://www.bleepingcomputer.com/news/security/neiman-marcus-confirms-data-breach-after-snowflake-account-hack/ (last visited Aug. 16, 2024).

[25] Jonathan Greig, *LendingTree Confirms That Cloud Services Attack Potentially Affected Subsidiary*, THE RECORD (June 10, 2024), https://therecord.media/lendingtree-quotewizard-cybersecurity-incident-snowflake. (last visited Aug. 16, 2024).

[26] *Id.*

[27] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26-38 (May 2015), https://www.researchgate.net/publication/283668023. (last visited Aug. 16, 2024). The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[28] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD No. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

companies have spent over $19 billion on acquiring personal data of consumers in 2018.[29] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Indeed, threat actors who compromised Defendant's systems are seeking millions of dollars in exchange for this Private Information.

51. Defendant is one of the largest digital warehouse providers in the United States and contracts with thousands of companies to securely store customers and employes' data on its Snowflake Data Cloud. As such, Defendant is responsible for developing and maintaining environments which collects and processes personal data for hundreds of millions of Americans.

52. Defendant collects, receives, and stores extensive individually identifiable information. Depending on its corporate clientele, these records include names, email and home addresses, social security numbers, IP and pixel tracking data, credit card information, auto insurance information and more. All data Snowflake's corporate clients seek to utilize in their day-to-day business operations is placed on Snowflake Data Clouds.

53. Defendant included privacy policies and commitments to maintain the confidentiality of data stored in their digital warehouses as terms of contracts with its corporate clients. Through contract terms and representations to its corporate clients and the public, Defendant promised to take specific measures to protect Private Information, as American companies sought to provide their customers with services utilizing their data, and as such, these customers were intended third-party beneficiaries of Defendant's contracts.

54. As such, Snowflake has failed to secure the Private Information of the individuals that provided their sensitive information to Ticketmaster and all other clients herein. Defendant failed to take appropriate steps to protect the PII of Plaintiffs and other Class Members from being disclosed.

III. Defendant Failed to Comply with FTC Guidelines

55. Defendant was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that a company's failure to maintain

[29] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/. (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

56. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[30] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[31]

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("**FTCA**"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their

[30] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited Aug. 16, 2024).

[31] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

data security obligations.

IV. Plaintiffs and the Class Have Suffered Injury as a Result of Defendant's Data Mismanagement

60. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiffs and Class Members' Private Information has been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiffs and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

61. Plaintiffs and Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

62. Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

63. As a result of Private Information's real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

64. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[32] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data

[32] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs//. (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

breaches from $900 to $4,500.[33]

65. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[34]

66. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

67. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.[35] The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that 1) cybercriminals are targeting large, public companies such as Snowflake; 2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; 3) cybercriminals were selling large volumes of Private Information and corporate information on Dark Web portals; 4) the threats were increasing.

68. Had Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

a. Lack of complete assessment, including internal, third-party, and cloud-based systems and services;

---

[33] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited Aug. 16, 2024).

[34] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1. (last visited Aug. 16, 2024).

[35] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

b. Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;

c. Misconfigured devices/servers;

d. Unencrypted data and/or poor encryption key management and safeguarding;

e. Use of end-of-life (and thereby unsupported) devices, operating systems and applications;

f. Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;

g. Failure to block malicious email; and

h. Users succumbing to business email compromise (BEC) and social exploits.[36]

69. Plaintiffs and Class Members must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

70. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendant's conduct. Further, the value of Plaintiffs and Class Members' Private Information has been diminished by its exposure in the Data Breach.

71. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

72. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of Defendant's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Private

[36] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/securityawareness/post/ota-report-indicates-93-security-breaches-are-preventable (last visited Aug. 16, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Information, a form of property that Defendant obtained from Plaintiffs; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

73. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm.

74. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Private Information.

75. Plaintiffs, individually and on behalf of all other similarly situated individuals, allege claims in negligence, negligence per se, breach of implied contract, unjust enrichment, violations of the California Consumer Privacy Act, and California's Unfair Competition Law.

CLASS ALLEGATIONS

76. **Class Definition:** Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure Sections 23(b)(2), 23(b)(3), and 23(c)(4), on behalf of Plaintiffs and the Class defined as follows:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach. ("**the Class**").

California Subclass

> All individuals residing in California whose Private Information was compromised as a result of the Data Breach. ("**the California Subclass**").

77. Collectively, the Class and California Subclass are referred to as the Classes.

78. Excluded from the Classes are Snowflake's officers and directors, and any entity in which Snowflake has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Snowflake. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

79. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

80. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable – millions of individuals have been affected by this Data Breach.

81. **Predominance of Common Questions**. There exist questions of law and fact common to the Class, which predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant was subject to (and breached) the FTC Act, and/or the CCPA;

g. Whether Defendant breached its duty to Class Members to safeguard their Private Information

h. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

i. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts breached an implied contract they formed with Plaintiffs and the Class Members;

l. Whether Defendant's acts breached Class Members' rights as third-party beneficiaries of Defendant's contracts with third parties;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

m. Whether Defendant was unjustly enriched to the detriment of Plaintiffs and the Class;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

82. **Adequacy**. Plaintiffs are adequate representatives for the Class because their interests do not conflict with the interests of the Class that they seek to represent. Plaintiffs have retained counsel competent and highly experienced in complex class action litigation counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their experienced counsel.

83. **Superiority**. A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and Class Members. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Defendant. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, inter alia, the records (including databases, e-mails, dealership records and files, etc.) Defendant maintains regarding Plaintiffs and Class Members.

84. Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CLAIMS FOR RELIEF

COUNT I

NEGLIENCE

(On Behalf of Plaintiffs and the Class)

85. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

86. Defendant owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control.

87. Defendant knew, or should have known, the risks of collecting and storing Plaintiffs and all other Class Members' Private Information and the importance of maintaining secure systems. Defendant knew, or should have known, of the vast uptick in data breaches in recent years. Defendant had a duty to protect the Private Information of Plaintiffs and Class Members.

88. Given the nature of Defendant's business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendant had a duty to prevent.

89. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiffs and Class Members' Private Information.

90. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs and Class Members' Private Information to unauthorized individuals.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

91. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

92. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II

NEGLIENCE PER SE

(On Behalf of Plaintiffs and the Class)

93. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

94. Defendant's duties arise from Section 5 of the FTC Act ("**FTCA**"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure Private Information.

95. Defendant violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs and all other Class Members' Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

96. Defendant's violations of Security Rules and Section 5 of the FTCA constitute negligence per se.

97. Plaintiffs and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

98. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

99. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs and Class Members' Private Information to unauthorized individuals.

100. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendant's violations of Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiffs and the Nationwide Class)

101. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

102. Plaintiffs and Class Members either directly or indirectly gave Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiffs and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs and Class Members' Private Information created a fiduciary relationship between Defendant and Plaintiffs and Class Members. Considering this relationship, Defendant must act primarily for the benefit of Plaintiffs and Class Members, which includes safeguarding and protecting Plaintiffs and Class Members' Private Information.

103. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs and Class Members' Private Information and failing to safeguard the Private Information of Plaintiffs and Class Members it collected.

104. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

106. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for services—namely, the provided and entrusted Defendant with their valuable

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Private Information. Defendant funds its data security measures entirely from payments made on behalf Plaintiffs and the Class Members who are the intended beneficiaries of a contract between Defendant and its corporate clients. Accordingly, a portion of such payments made on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is to be allocated to data security is known to Defendant.

107. In exchange for their payment, Plaintiffs and Class Members were entitled to reasonable measures to protect their Private Information.

108. Defendant appreciated, accepted and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein –namely, (a) Plaintiffs and Class members conferred a benefit on Defendant, and Defendant accepted or retained that benefit; and (b) Defendant used Plaintiffs and Class Members' Private Information for business purposes.

109. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit provided on behalf of Plaintiffs and Class Members.

110. Defendant acquired the Private Information through inequitable means in that it failed to disclose its inadequate security practices previously alleged.

111. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

112. Under the circumstances, it would be unjust and unfair for Defendant to be permitted to retain any of the benefits conferred on behalf of Plaintiffs and the Class.

113. Under the principles of equity and good conscience, Defendant should not be permitted to retain the Private Information belonging to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures that industry standards mandate.

114. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received on behalf of and for the benefit of Plaintiffs and the Class.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT V

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Class)

115. Plaintiffs reallege and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

116. Defendant required Plaintiffs and Class Members to provide or authorize the transfer of their Private Information for Defendant to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs and Class Members' Private Information and to timely notify them in the event of a data breach.

117. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

118. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

119. Defendant breached the implied contracts by failing to safeguard Plaintiffs and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

120. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

COUNT VI

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

(On Behalf of Plaintiffs and the Class)

121. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

122. Defendant entered into contracts with its various corporate clients (like Ticketmaster, Advanced Auto Parts and other entities) to provide data storage services and maintain data cloud

secure data cloud systems for the cu, made expressly for the benefit of Plaintiffs and Class members, who were customers and/or employees of at least one of the contracting parties. In order to effectuate offered services (i.e., ticket sales, auto insurance, retail purchases), and upon information and belief as to the exact terms of the contract, Defendant agreed to collect, store, and protect Plaintiffs and Class Members' Private Information.

123. Thus, the benefit of collection, protection, and storage of the Private Information was the direct, intended, and primary objective of the contracting parties.

124. Defendant breached its contract with its corporate clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs and Class Members' Private Information.

125. Defendant knew that if it were to breach its contracts, the harm would befall its clients' customers and employees for whom the benefit was intended to confer. As such, Defendant's failures to uphold the terms of its contract and allow for the Data Breach that has foreseeably harmed Plaintiffs and the Class.

126. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs including attorneys' fees incurred.

COUNT VII

VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Cal. Civ. Code §§ 1798.100 et seq. ("CCPA")

(On Behalf of the California Subclass)

127. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

128. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

129. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

130. Defendant is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

131. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

132. Plaintiffs are "consumers" as defined by Civ. Code § 1798.140(g) because they are natural persons residing in the state of California.

133. Defendant is a "business" as defined by Civ. Code § 1798.140(c).

134. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." See Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

135. Plaintiffs' Private Information compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

136. Through the Data Breach, Plaintiffs' private information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

137. The Data Breach occurred because of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

138. Simultaneously herewith, Plaintiffs are providing notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiffs allege

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Defendant has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Defendant is unable to cure or do not cure the violation within 30 days, Plaintiffs will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

139. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VIII

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL")

(On Behalf of the California Subclass)

140. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

141. Plaintiffs bring this claim on behalf of themselves and the California Class.

142. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("**UCL**"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

143. By reason of Defendant's above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class Members' Private Information, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

144. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the private and confidential Private Information of Plaintiffs and the Class has been compromised for all to see, use, or otherwise exploit.

145. Defendant's practices were unlawful and in violation of the laws discussed herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

146. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive Plaintiffs and the Class into believing that the Private Information, they provide to Defendant will remain private and secure, when in fact it was not private and secure.

147. Plaintiffs and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their Private Information.

148. Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 et seq., in that Defendant's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

149. But for Defendant's misrepresentations and omissions, Plaintiffs and Class Members would not have provided their Private Information to Defendant or its corporate clients or would have insisted that their Private Information be more securely protected.

150. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information, they have been injured as follows: (1) the loss of the opportunity to control how their Private Information is used; (2) the diminution in the value and/or use of their Private Information entrusted to Defendant; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their Private Information; and (5) costs associated with monitoring their Private Information, amongst other things.

151. Plaintiffs take upon themselves enforcement of the laws violated by Defendant in connection with the reckless and negligent disclosure of Private Information. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the Proposed Class that they seek to represent, respectfully requests the following relief:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For an order granting permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

i. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs and Class Members' Private Information;

ii. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct automated security monitoring and testing, including simulated attacks, penetration tests, and audits on Defendant systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. Requiring Defendant to delete, destroy and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. Requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

v. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's networks is compromised,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

hackers cannot gain access to other portions of Defendant's systems;

vi. Requiring Defendant to conduct regular database scanning and securing checks;

vii. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

viii. Requiring Defendant to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. Requiring Defendant to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting Private Information;

x. Requiring Defendant to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. Requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xii. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from its clients' servers;

xiii. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Defendant's compliance with the terms of the Court's final judgment, to provide

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment; and

xiv. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein.

C. For an order requiring Defendant to pay for credit monitoring services for Plaintiffs and the Class of a duration to be determined at trial;

D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

DATED: August 16, 2024

CLARKSON LAW FIRM, P.C.

/s/ Ryan J. Clarkson

Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (CA SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood (SBN 149343)
tblood@bholaw.com
Jennifer L. MacPherson (SBN 202021)
jmacpherson@bholaw.com
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100

COTCHETT, PITRE & McCARTHY LLP
Thomas E. Loeser (SBN 202724)
tloeser@cpmlegal.com
Karin B. Swope (*PHV forthcoming*)
kswope@cpmlegal.com
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577

ROSSBACH LAW, P.C.
William A. Rossbach (SBN 1338)
bill@rossbachlaw.com
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Tel: (406) 543-5156
Fax: 619-338-1101

Counsel for Plaintiffs and the Proposed Class

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com